Indag. Mathem., N.S., 12 (4), 477–482 December 17, 2001

A Diophantine equation appearing in Diophantine approximation

by Yuan Jin and Asmus L. Schmidt

Department of Mathematics, Northwest University, Xi'an 710069, P.R. China
Department of Mathematics, Universitetsparken 5, DK-2100 Copenhagen, Denmark

Communicated by Prof. R. Tijdeman at the meeting of September 24, 2001

ABSTRACT

All Diophantine equations

$$ax^2 + by^2 + cz^2 = 1 + dxyz, \quad \text{with} \quad a, b, c, d \in N \quad \text{and} \quad a|d,\ b|d,\ c|d,$$

having solutions $(x, y, z) \in N^3$ are determined. One particular equation of this type

$$2x^2 + 2y^2 + 3z^2 = 1 + 6xyz$$

appeared recently in connection with the description of the lower part of the approximation spectrum for quaternions.

Recently the Diophantine equation

$$2x^2 + 2y^2 + 3z^2 = 1 + 6xyz$$

appeared in connection with the description of the lower part of the approximation spectrum for quaternions [3], but also the same equation is connected with the description of approximation constants for complex numbers on the circle $\{z \in C \mid |z| = 1/\sqrt{2}\}$ with respect to integers in the field $Q(\sqrt{-3})$. Analogous results are to be expected in general with other circles in the complex plane and integers of an imaginary quadratic number field, especially when the circle contains no points from the number field.

With this motivation we will consider the Diophantine equation

$$(1) \qquad ax^2 + by^2 + cz^2 = 1 + dxyz, \quad \text{with } a, b, c, d \in N \text{ and } a|d,\ b|d,\ c|d,$$

and we look for (a, b, c, d), where (1) has a solution $(x, y, z) \in N^3$.

Clearly $\gcd(a, b, c) = 1$. We let

$$L = \{(x, y, z) \in N^3 \mid ax^2 + by^2 + cz^2 = 1 + dxyz\},$$

and we notice that if $(x, y, z) \in L$ then

$$\begin{aligned} \Psi_1(x, y, z) &= \big((d/a)yz - x, y, z\big) \in L, \\ \Psi_2(x, y, z) &= \big(x, (d/b)xz - y, z\big) \in L, \\ \Psi_3(x, y, z) &= \big(x, y, (d/c)xy - z\big) \in L. \end{aligned}$$

The three solutions $\Psi_j(x, y, z)$ are called *neighbouring* solutions to (x, y, z). A solution $(x, y, z) \in L$ with

$$1 \le x \le d/(2a)yz, \quad 1 \le y \le d/(2b)xz, \quad 1 \le z \le d/(2c)xy,$$

is called a *fundamental* solution. With $h(x, y, z) = x + y + z$ as *height* function, a fundamental solution (x, y, z) has height $\le$ the height of its three neighbours. By arguments analogous to those in [1], [2] every solution to (1) comes through the neighbouring process from a unique fundamental solution.

If precisely one of the coefficients a, b, c in (1), say c, is divisible by p^2, where p is a prime, then any solution (x_0, y_0, z_0) to (1) comes from a solution (x_0, y_0, pz_0) to

$$(1') \qquad ax^2 + by^2 + c'z^2 = 1 + d'xyz, \quad \text{where } c' = c/p^2, \; d' = d/p.$$

If two of the coefficients a, b, c in (1), say b and c, are divisible by f^2, where $f > 1$, then any solution (x_0, y_0, z_0) to (1) comes from a solution (x_0, fy_0, fz_0) to

$$(1'') \qquad ax^2 + b''y^2 + c''z^2 = 1 + d''xyz, \quad \text{where } (b'', c'', d'') = (b, c, d)/f^2.$$

Since the equations $(1')$ and $(1'')$ are of the same type as (1), and a fundamental solution to (1) comes from fundamental solutions to $(1')$ or $(1'')$, it follows that it is enough to consider equations (1) which are *primitive* in the sense that a, b, c are all squarefree.

Theorem. *Let $a, b, c, d \in N$ with $a|d$, $b|d$, $c|d$ and $\gcd(a, b, c) = 1$, and assume that the equation* (1) *is primitive and has a fundamental solution (x, y, z). Then apart from a permutation of $((a, x), (b, y), (c, z))$ one of the following cases (with b squarefree in case* 4*) must occur:*

case	a	b	c	d	(x, y, z)
1	5	1	5	5	$(1, 4, 2)$ *or* $(2, 4, 1)$
2	3	1	6	6	$(1, 2, 1)$
3	7	2	14	14	$(1, 2, 1)$
4	1	b	b	$2b$	$(1, t, t), t \in N$
5	2	2	3	6	$(1, 1, 1)$
6	6	10	15	30	$(1, 1, 1)$
7	2	1	2	2	$(2, 3, 2)$

Proof. Let

$$x' = \sqrt{a}x, \quad y' = \sqrt{b}y, \quad z' = \sqrt{c}z, \quad d' = d/\sqrt{abc}.$$

Then

$$(2) \qquad x'^2 + y'^2 + z'^2 = 1 + d'x'y'z'.$$

By symmetry we may assume that

$$(3) \qquad 1 \leq x' \leq \min(y', z').$$

In case $y' \leq z'$ we rewrite (2) into

$$(d'x'y' - 2z')^2 = d'^2x'^2y'^2 - 4x'^2 - 4y'^2 + 4,$$

and since $2cz \leq dxy$ and hence $2z' \leq d'x'y'$ we have

$$y' \leq z' = \frac{1}{2}d'x'y' - \frac{1}{2}\sqrt{d'^2x'^2y'^2 - 4x'^2 - 4y'^2 + 4}$$

which implies

$$\sqrt{d'^2x'^2y'^2 - 4x'^2 - 4y'^2 + 4} \leq d'x'y' - 2y',$$

giving

$$d'x'y'^2 \leq x'^2 + 2y'^2 - 1 \leq 3y'^2 - 1 < 3y'^2.$$

Thus $d'x' < 3$ or equivalently $(d/b)(d/c)x^2 < 9$. The case $z' \leq y'$ leads similarly to the same result. On the other hand the quadratic form

$$f(y, z) = by^2 + cz^2 - (dx)yz (= 1 - ax^2)$$

represents $b, c > 0$ and $1 - ax^2 \leq 0$, hence

$$\operatorname{discr}(f) = (dx)^2 - 4bc = bc((d/b)(d/c)x^2 - 4) \geq 0,$$

so that $(d/b)(d/c)x^2 \geq 4$. Altogether we must have

$$(4) \qquad 4 \leq (d/b)(d/c)x^2 < 9.$$

By symmetry we may assume additionally that $b \leq c$. Hence by (4) either

$$x = 1 \text{ and } (d/b, d/c) \in \{(4,1), (5,1), (6,1), (7,1), (8,1), (2,2), (3,2), (4,2)\},$$

or

$$x = 2 \text{ and } (d/b, d/c) \in \{(1,1),(2,1)\}.$$

Notice first that $x = 1$ and $(d/b, d/c) \in \{(4,1),(8,1)\}$ can not occur by the assumption of primitivity. The remaining 8 possibilities are considered separately.

1) $x = 1$, $c = d = 5b$. Since $\gcd(a,b,c) = 1$ and $a|d$ we have $a = 1$ or $a = 5$. Thus (1) becomes

$$ax^2 + by^2 + 5bz^2 = 1 + 5bxyz, \text{ where } a \in \{1,5\} \text{ and } x = 1.$$

Hence $b(y^2 + 5z^2 - 5yz) = 1 - a \in \{0, -4\}$. Clearly only the second option is possible leading to case 1: $(a,b,c,d) = (5,1,5,5)$ with fundamental solution $(x,y,z) = (1,4,2)$. Notice that $b = 4$ is impossible by the assumption of primitivity, and that $b = 2$ is impossible since $y^2 + 5z^2 - 5yz = -2$ is unsolvable modulo 5.

2) $x = 1$, $c = d = 6b$. Since $\gcd(a,b,c) = 1$ and $a|d$ we have $a \in \{1,2,3,6\}$. Thus (1) becomes

$$ax^2 + by^2 + 6bz^2 = 1 + 6bxyz, \text{ where } a \in \{1,2,3,6\} \text{ and } x = 1.$$

Hence $b((y-3z)^2 - 3z^2) = 1 - a \in \{0,-1,-2,-5\}$. Clearly $(y-3z)^2 - 3z^2 = 0$ is impossible, but also $(y-3z)^2 - 3z^2 = -1$ is impossible modulo 3. Therefore it remains to consider

$$(b = 1 \text{ and } (y-3z)^2 - 3z^2 = -2) \text{ or } (b = 1 \text{ and } (y-3z)^2 - 3z^2 = -5).$$

Since $(y-3z)^2 - 3z^2 = -5$ is unsolvable, we find only case 2: $(a,b,c,d) = (3,1,6,6)$ with fundamental solution $(x,y,z) = (1,2,1)$.

3) $x = 1$, $c = d = 7b$. Since $\gcd(a,b,c) = 1$ and $a|d$ we have $a \in \{1,7\}$. Thus (1) becomes

$$ax^2 + by^2 + 7bz^2 = 1 + 7bxyz, \text{ where } a \in \{1,7\} \text{ and } x = 1.$$

Hence $b(y^2 + 7z^2 - 7yz) = 1 - a \in \{0,-6\}$. Clearly $y^2 + 7z^2 - 7yz = 0$ is impossible. Also $y^2 + 7z^2 - 7yz = -6$ is seen to to be unsolvable by considering it modulo 3 and modulo 9. Further $y^2 + 7z^2 - 7yz \equiv -1 \pmod 7$ and $y^2 + 7z^2 - 7yz \equiv -2 \pmod 7$ are impossible. Therefore it remains to consider

$$b = 2 \text{ and } y^2 + 7z^2 - 7yz = -3,$$

which leads to case 3: $(a,b,c,d) = (7,2,14,14)$ with fundamental solution $(x,y,z) = (1,2,1)$.

4) $x = 1$, $c = b$, $d = 2b$. Since $\gcd(a,b,c) = 1$ and $a|d$ we have $a \in \{1,2\}$. Thus (1) becomes

$$ax^2 + by^2 + bz^2 = 1 + 2bxyz, \text{ where } a \in \{1,2\} \text{ and } x = 1.$$

Hence $b(y-z)^2 = 1 - a \in \{0,-1\}$. This is only possible if $a = 1$, and leads to case 4: $(a,b,c,d) = (1,b,b,2b)$ with fundamental solutions $(x,y,z) = (1,t,t)$, $t \in N$.

5) $x = 1$, $2c = 3b$, $d = 3b$. Since $\gcd(a, b, c) = 1$ and $a|d$ we have $a \in \{1, 2, 3, 6\}$. Thus (1) becomes

$$ax^2 + by^2 + \frac{3}{2}bz^2 = 1 + 3bxyz, \text{ where } a \in \{1, 2, 3, 6\} \text{ and } x = 1,$$

where $b = 2\tilde{b}$ is even. Hence $\tilde{b}(2y^2 + 3z^2 - 6yz) = 1 - a \in \{0, -1, -2, -5\}$. Clearly $2y^2 + 3z^2 - 6yz = 0$ is impossible, but also $2y^2 + 3z^2 - 6yz \equiv -2 \equiv -5 \pmod 3$ is impossible. Therefore it remains to consider

$$\tilde{b} \in \{1, 2, 5\} \text{ and } 2y^2 + 3z^2 - 6yz = -1,$$

which leads to case 5: $(a, b, c, d) = (2, 2, 3, 6)$ with fundamental solution $(x, y, z) = (1, 1, 1)$, and to case 6: $(a, b, c, d) = (6, 10, 15, 30)$ with fundamental solution $(x, y, z) = (1, 1, 1)$. The possibility $\tilde{b} = 2$ gives $b = 4$ and is therefore excluded by the assumption of primitivity.

6) $x = 1$, $c = 2b$, $d = 4b$. Since $\gcd(a, b, c) = 1$ and $a|d$ we have $a \in \{1, 2, 4\}$, and indeed $a \in \{1, 2\}$ by the assumption of primitivity. Thus (1) becomes

$$ax^2 + by^2 + 2bz^2 = 1 + 4bxyz, \text{ where } a \in \{1, 2\} \text{ and } x = 1.$$

Hence $b(y^2 - 2(y - z)^2) = a - 1 \in \{0, 1\}$. Since $y^2 - 2(y - z)^2 = 0$ is impossible it remains to consider $b = a - 1 = 1$ and $y^2 - 2(y - z)^2 = 1$, which leads to $(a, b, c, d) = (2, 1, 2, 4)$ with fundamental solution $(x, y, z) = (1, 1, 1)$. However this does not satisfy (3) and is therefore omitted (cf. case 4 with $b = 2$).

7) $x = 2$, $b = c = d$. Since $\gcd(a, b, c) = 1$ and $a|d$ we have $a = 1$. Thus (1) becomes

$$x^2 + by^2 + bz^2 = 1 + bxyz, \text{ where } x = 2.$$

Hence $b(y - z)^2 = -3$, which is impossible.

8) $x = 2$, $c = d = 2b$. Since $\gcd(a, b, c) = 1$ and $a|d$ we have $a \in \{1, 2\}$. Thus (1) becomes

$$ax^2 + by^2 + 2bz^2 = 1 + 2bxyz, \text{ where } a \in \{1, 2\} \text{ and } x = 2.$$

Hence it remains to consider the two possibilities

$$(b = 1 \text{ and } y^2 - 2(y - z)^2 = 3) \text{ or } (b = 3 \text{ and } y^2 - 2(y - z)^2 = 1), \tag{5}$$

$$(b = 1 \text{ and } y^2 - 2(y - z)^2 = 7) \text{ or } (b = 7 \text{ and } y^2 - 2(y - z)^2 = 1). \tag{6}$$

By considering congruences modulo 3 and modulo 9 we can exclude the first option in (5). The second option in (5) leads to $(a, b, c, d) = (1, 3, 6, 6)$ with fundamental solution $(x, y, z) = (2, 1, 1)$, thus this does not satisfy (3) and is therefore omitted (cf. case 2).

The first option in (6) leads to case 7: $(a, b, c, d) = (2, 1, 2, 2)$ with fundamental solution $(x, y, z) = (2, 3, 2)$. The second option in (6) leads to $(a, b, c, d) = (2, 7, 14, 14)$ with fundamental solution $(x, y, z) = (2, 1, 1)$, thus this does not satisfy (3) and is therefore omitted (cf. case 3).

REFERENCES

[1] Hurwitz, A. – Über eine Aufgabe der unbestimmten Analysis. Archiv der Math. und Phys. **14**, 185–196 (1907).

[2] Rosenberger, G. – Über die Diophantische Gleichung $ax^2 + by^2 + cz^2 = dxyz$. J. reine angew. Math. **305**, 122–125 (1979).

[3] Schmidt, A.L. – Diophantine approximation of quaternions. To appear.

(Received July 2001)